

# UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF TEXAS

United States Courts  
Southern District of Texas  
FILED  
JAN 09 2019  
David J. Bradley, Clerk of Court

In the Matter of the Search of:

**111 ROSEWOOD STREET  
LAKE JACKSON, TX 77566**

## APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: **G-19-002**

I, **John Estes**, being duly sworn depose and say:

I am a **Special Agent with U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI)** and have reason to believe that on the property or premises known as **111 Rosewood Street, Lake Jackson, TX 77566**, more particularly described in *Attachment A* affixed hereto

in the Southern District of Texas, there is now concealed a certain person or property, namely  
(See Attachment B)

which is **1) evidence of the commission of a crime; 2) property designed or intended for use or which is or has been used as the means of committing a criminal offense and 3) contraband, controlled substances,**

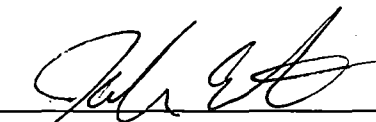
concerning a violation of Title 21 United States Code, Section 841(a)(1) and 846.

The facts to support a finding of Probable Cause are as follows:

Your Affiant, **John Estes**, is a Special Agent with U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI), and has been employed by HSI as such since 2008.

(See Attachment C, Sworn Statement of Special Agent John Estes)

Continued on the attached sheet and made a part hereof: ☒ Yes ☐ No



Signature of Applicant  
**John Estes**

Sworn to before me and subscribed in my presence,

1-9-18

Date

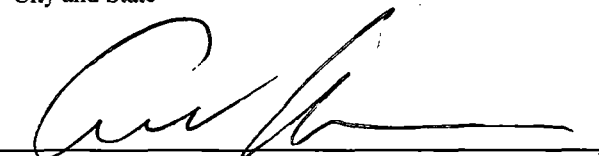
at

Galveston, Texas

City and State

*United States Magistrate Judge  
Aaron Edison*

Name & Title of Judicial Officer



Signature of Judicial Officer

**ATTACHMENT A****DESCRIPTION OF ITEMS TO BE SEARCHED**

The residence, 111 Rosewood Street, Lake Jackson, Texas 77566 is a red brick house facing east on Rosewood Street between two residences labeled 109 and 113. The residence also includes all curtilage, outbuildings, and at least one vehicle, a 2007 Dodge Ram pickup bearing Texas plate DMX9996, which returns to Jason PHILLIPS. Photos of the residence are included below for the purpose of identification of the premises.



**ATTACHMENT B**

**DESCRIPTION OF PROPERTY TO BE SEIZED**

1. Controlled substances, pills, tablets, or gel capsules
2. Any and all evidence, fruits, and instrumentalities of violations of controlled substance trafficking. Identification documents including: fraudulent identification documents and legitimate identification documents;
3. Computers, laptops, tablets, cellphones, smart phones, removable or remote storage media, writeable or rewritable CD's and DVD's, or any other device located within the premises capable of accessing the internet;
4. Narcotics trafficking and transaction records, including: customer lists and ledgers of narcotics transactions;
5. Currency;
6. Financial records relating to moneys derived from illegal narcotics trafficking including: money transfer receipts; and other evidence of financial transactions relating to obtaining, transferring, secreting or spending various sums of money derived from engaging in narcotics trafficking activities;
7. Cellular telephone records including: bills, both current and past; service agreements and activations; and applicable telephone charging cables and other accessories;
8. Indicia of residence or ownership including: rental bills or mortgage statements; utility bills, both current and past.

**ATTACHMENT C**

**SWORN STATEMENT IN SUPPORT OF SEARCH WARRANT APPLICATION**

**INTRODUCTION**

1. I am a Special Agent of the United States Department of Homeland Security and have been so appointed since 2008. I have personally conducted or assisted in numerous investigations of criminal violations of the Controlled Substances Act and other violations of Federal law.

**PURPOSE OF THE AFFIDAVIT**

2. This affidavit is submitted in support of applications for a search warrant for 111 Rosewood Street Lake Jackson, TX 77566. The location, 111 Rosewood Street, Lake Jackson, TX 77566 is further described in Attachment A and incorporated herein.
3. Based on evidence I have reviewed in this investigation, coupled with information I have received from other law enforcement personnel involved in this investigation, I believe that located at 111 Rosewood Street, Lake Jackson, TX 77566, there will be evidence, as described in "Attachment B" of this affidavit. I believe this evidence will be useful in furthering this investigation. I have not set forth each and every fact known to me in this investigation, only those facts and circumstances necessary to establish probable cause for the requested warrant.

**TRAINING AND EXPERIENCE**

4. As previously stated, I have been employed by the United States Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) since 2008. I have received specialized training from Federal Law Enforcement Training Center. This training, in part, focused on methods of unlawful drug trafficking, the

identification of controlled substances, the means by which drug traffickers derive, launder, and conceal their profits, the use of assets to facilitate unlawful drug trafficking activity, and laws permitting the forfeiture to the United States of assets purchased with drug proceeds or assets used or intended to be used to facilitate drug violations.

5. I have participated in the execution of search warrants while investigating drug traffickers and drug trafficking organizations. These warrants covered the search of locations including residences of drug traffickers, their co-conspirators, associates, as well as drug processing operations and stash houses used as storage and distribution points for controlled substances.
6. Materials searched for and recovered in the locations I have searched include (a) various controlled substances (b) drug paraphernalia such as scales, papers and drug packaging materials, (c) books, ledgers, drug customer lists and records reflecting sales, the transfer or transportation of drugs and amounts of monies owed for drugs, (d) records reflecting the names, addresses, and telephone numbers of co-conspirators, (e) sales receipts and other records reflecting the expenditure of monies that are the proceeds from unlawful drug distribution, (e) records of banking transactions to conceal and launder drug trafficking proceeds, and (f) various valuable assets purchased with the proceeds of unlawful drug trafficking. These items constituted evidence of drug offenses in violation of 21 U.S.C. § 841, 846, and 952, acquisition of assets with drug trafficking proceeds and the use of these assets to facilitate drug trafficking crimes in violation of 21 U.S.C. § 853, as well as violations of tax and money laundering statutes.
7. Based upon training, experience, and participation in this and other drug trafficking investigations, I have reason to believe that:
  - a) drug traffickers often maintain in their residences and/or business establishment records relating to the transportation, ordering, sale and distribution of controlled substances and the outstanding debts and collections from controlled substances that

have been distributed including some or all of the following: electronically stored data, computerized or written books, bank records, receipts, diaries, notes, ledgers, airline tickets, cashier's checks, money order receipts, and other papers. Furthermore, I know that drug traffickers often retain these records as they are often coded in nature and might appear innocuous to the untrained investigator;

- b) drug traffickers commonly provide their illegal drugs on consignment sale to their customers, who subsequently pay for the drugs after reselling the product. Therefore, the above-mentioned books, records, receipts, notes, ledgers, etc., will be secured by the drug traffickers within their residences and/or their businesses for their ready access to them for the purpose of determining drug debts and collecting monies derived from the sale of drugs;
- c) drug traffickers must maintain and/or have quick access to large amounts of United States currency or other liquid assets in order to maintain and finance their ongoing drug business;
- d) drug traffickers commonly conceal contraband, proceeds of drug transactions, records of these transactions, and records reflecting names, nicknames, addresses and telephone numbers of drug associates within their residence and/or place of business, for ready access and to hide them from law enforcement agencies;
- e) drug traffickers commonly will attempt to legitimize the profits from illegal drug transactions by using domestic banks and their attendant services (i.e., safe deposit boxes, securities, cashier's checks, money drafts, letters of credit, brokerage houses, real estate, shell corporations and business fronts);
- f) drug traffickers often have photographs or video movies of themselves, their co-conspirators and the property and assets purchased with drug proceeds. These photographs and video movies are normally in the drug traffickers' possession, their residence and/or their place of business;

- g) drug traffickers' methods of transporting drugs include but are not limited to: commercial airlines, private motor vehicles, and government and contract mail carriers. I know that the residences of drug traffickers will often contain records of drug-related travel. These records may include airline ticket receipts, credit card receipts, rental car receipts and luggage tags reflecting points of travel;
- h) drug traffickers commonly have firearms in their possession (on their person, at their residence, and/or their business) including handguns, rifles, shotguns and automatic weapons. These firearms are most often used and/or maintained in order to protect and secure a drug trafficker's property or manufacturing operation;
- i) drug traffickers will often accumulate and maintain substantial amounts of drug proceeds, specifically currency, over a period of years, so that the proceeds can be used in later years for personal asset acquisitions and/or expenditures during periods when a drug trafficker is not distributing drugs;
- j) drug traffickers commonly have evidence of purchases of their drugs secreted in their residences;
- k) drug traffickers commonly secrete in their residences, over a period of years, items such as those identified in the above paragraphs;
- l) it is common for individuals who order illegal controlled substances from an international distributor to utilize computers and/or other electronic devices to access the internet in order to research and order the controlled substance, as well as to communicate with other potential co-conspirators. International orders of controlled substances are commonly made via the internet websites both on the surface web or via dark web marketplaces. Commonly the sender of the controlled substances and intended recipient of such orders are not known to one another personally and transactions are commonly conducted utilizing wire transfers, money orders, credit or debit payments, digital currency, or cryptocurrency.

8. A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet including websites, social media sites, bulletin boards, file sharing, and other Internet sites. Wireless telephones often have a subscriber identity module or subscriber identification module (“SIM”), which is an integrated circuit that securely stores the International Mobile Subscriber Identity (“IMSI”) and the related key used to identify and authenticate subscribers on mobile telephone devices. A SIM is embedded into a removable “SIM card,” which can be transferred between different mobile devices. A SIM card contains a unique serial number (“ICCID”), IMSI, security authentication and ciphering information, temporary information related to the local network, a list of the services to which the user has access, and certain passwords. Most SIM cards will also store certain usage data, such as call history, text (“SMS”) messages, and phone book contacts. Wireless telephones may also be “smartphones,” such that they operate as personal computers capable of accessing the Internet. They may also include GPS technology for determining the location of the device. Such telephones may also contain removable storage media, such as a flash card—such devices can store any digital data and can have the capacity to store many gigabytes of data. Some cellular telephones also have software, giving them the same capabilities as personal computers including accessing and editing word processing documents, spreadsheets, and presentations. Some cellular telephones also operate as a

“tablet,” or mobile computer, and can contain software programs called applications. Those programs can perform different functions and save data associated with those functions, including use associated with the Internet.

9. A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called applications (“apps”), which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
10. A hard disk drive (“HDD”), also known as a hard drive or hard disk, is a data storage device that consists of an external circuit board, external data, power connections, and internal glass, ceramic, or magnetically charged rotating metal platters that permanently store data even when powered off. A solid-state drive (“SSD”), also known as a solid-state disk, is a data storage device that uses integrated circuit assemblies as memory to permanently store data instead of using rotating platters. Flash drives, flash cards, and thumb drives are digital storage devices that can connect to computers or other devices using the appropriate connection. CDs/DVDs are digital storage devices capable of storing large amounts of digital data—a user can store information onto a CD/DVD by “burning” digital data to the device using a computer CD/DVD drive. These devices are capable of storing any electronic information including images, videos, word processing documents, programs and software, and web pages.
11. Computers and digital storage devices can include all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptop computers, mobile phones, pagers,

tablets, server computers, game consoles, and network hardware and also includes any physical object upon which computer data can be recorded such as hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical media.

12. Based on my knowledge, training, and experience, I know that computers and digital storage devices can store information for long periods of time. Similarly, things that have been searched for and viewed via the Internet are typically stored for some period of time on a device. This information can sometimes be recovered with forensic tools.
13. Based on my knowledge, training, and experience, examining data stored on computers and digital storage devices can uncover, among other things, evidence that reveals or suggests who possessed or used the computer or digital storage devices.
14. There is probable cause to believe that things that were once stored on the Device(s) may still be stored there, for at least the following reasons:
15. Based on my knowledge, training, and experience, I know that digital files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a digital storage device or computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
16. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for

long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

17. Wholly apart from user-generated files, computer storage media including digital storage devices and computers' internal hard drives can contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
18. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." Forensic review may also disclose when and by whom the Internet was used to conduct searches, view material, and communicate with others via the Internet.
19. Though some communication applications and programs, such as Skype, retain little in the way of content of previous conversations but do retain records of use. Records can include registry records of times the program is in active use, times a call or conversation is initiated or received, or times a call or conversation is terminated.
20. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information on the Device(s) that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device(s) were used, the purpose of the use, who used the Device(s), and when. There

is probable cause to believe that this forensic electronic evidence might be on the Device(s) because:

21. Data on the storage medium can provide evidence of a file that was once on the storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer or device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created. This information can be recovered months or even years after they have been downloaded onto the storage medium, deleted, or viewed.
22. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
23. A person with appropriate familiarity with how a digital storage device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
24. The process of identifying the exact electronically stored information on storage media that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators.

Whether data stored on a computer is evidence may depend on other information stored on the computer or digital storage device and the application of knowledge about how a computer or digital storage device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

25. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
26. I know that when an individual uses an electronic device to aid in the commission of a crime, particularly the unlawful importation and distribution of controlled substances, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain evidence of online conversations with overseas persons involved in the distribution of controlled substances, visits to webpages that are involved in the distribution of controlled substances, text messages and phone conversations with persons involved in the distribution of controlled substances, records of controlled substance transactions, and disposition of funds derived from the sale of controlled substances.
27. I also know that those who engage in criminal activity will attempt to conceal evidence of the activity by hiding files, by renaming the format, (such as saving a .pdf image file as a .doc document file) or by giving them deceptive names such that it is necessary to view the contents of each file to determine what it contains.

28. I also know a single compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Thumb drives with a capacity of 32 gigabytes are not uncommon. Flash drives with a capacity of 32 gigabytes are not uncommon. Hard drives with the capacity of 500 gigabytes up to 3 terabytes are not uncommon. These drives can store thousands of images and videos at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with video capture capabilities, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.
29. I recognize the prudence requisite in reviewing and preserving in its original form only such records applicable to the violations of law described in this Affidavit and in Attachment B in order to prevent unnecessary invasion of privacy and overbroad searches. I believe it would be impractical and infeasible for the Government to review the mirrored images of digital devices that are copied as a result of a search warrant issued pursuant to this Application during a single analysis. I have learned through practical experience that various pieces of evidence retrieved from digital devices in investigations of this sort often have unknown probative value and linkage to other pieces of evidence in the investigation until they are considered within the fluid, active, and ongoing investigation of the whole as it develops. In other words, the weight of each individual piece of the data fluctuates based upon additional investigative measures undertaken, other documents under review and incorporation of evidence into a consolidated whole. Analysis is content-relational, and the importance of any associated data may grow whenever further analysis is performed. The full scope and meaning of the whole of the data is lost if each piece is observed individually, and not in sum. Due to

the interrelation and correlation between pieces of an investigation as that investigation continues, looking at one piece of information may lose its full evidentiary value if it is related to another piece of information, yet its complement is not preserved along with the original. In the past, I have reviewed activity and data on digital devices pursuant to search warrants in the course of ongoing criminal investigations. I have learned from that experience, as well as other investigative efforts, that multiple reviews of the data at different times is necessary to understand the full value of the information contained therein, and to determine whether it is within the scope of the items sought in Attachment B. In order to obtain the full picture and meaning of the data from the information sought in Attachments A and B of this application, the Government would need to maintain access to all of the resultant data, as the completeness and potential of probative value of the data must be assessed within the full scope of the investigation. As such, I respectfully request the ability to maintain the whole of the data obtained as a result of the search warrant, and to maintain and to review the data in the control and custody of the Government and law enforcement at times deemed necessary during the investigation, rather than minimize the content to certain communications deemed important at one time. As with all evidence, the Government will maintain the evidence and mirror images of the evidence in its custody and control, without alteration, amendment, or access by persons unrelated to the investigation.

30. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, copying and reviewing the contents of the Device(s) consistent with the warrant. The warrant I am applying for would authorize a later examination and perhaps repeated review of the device(s) or information from a copy of the Device(s) consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device(s) to human inspection in order to determine whether it is evidence described by the warrant. In the event any electronic devices are encountered within the

residence in a locked condition, submission of biometric identification, such as a fingerprint, may be necessary to unlock the device(s) for examination. The warrant I am applying for would compel any identified owner of a device in a locked condition to submit biometric identification to a device for unlock.

### **APPLE AND TOUCH ID**

31. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices, such as iPhones and iPads, offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, “fingerprint”) in lieu of a numeric, or alphanumeric, passcode or password. This feature is called Touch ID.
32. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center on the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering the passcode, as well as a more secure way to protect the device’s contents. This is particularly true when the user of the device is engaged in criminal activities and thus has a heightened concern about securing the contents of the device.

33. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made.
34. In my training and experience, the person who is in possession of a device, or has the device among his or her belongings at the time the device is found, is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the PREMISES to press their finger(s) against the Touch ID sensor

of the locked Apple device(s) found during the search of the PREMISES in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID.

### **BACKGROUND OF THE INVESTIGATION**

35. On February 23, 2018, HSI Special Agent (SA) John Estes and SA Laura Elder were notified by HSI Memphis of a large shipment intercepted inbound from China. The shipment was inspected and found to contain a mixture of Testosterone Propionate (a Schedule III Controlled Substance), Tadalafil (an uncontrolled prescription medication), and Sildenafil (an uncontrolled prescription medication) tablets destined to Laramie, Wyoming. The shipment was estimated, by weight, to contain approximately 11,030 tablets. The shipment was addressed to Fred WEEMS at 2373 Jefferson Street, Laramie, WY 82070 (hereafter Seized Shipment 1). SA Estes requested Seized Shipment 1 be forwarded to him in Cheyenne.
36. On March 7, 2018, SA Elder received notification from HSI Memphis of another shipment of an additional approximately 23,652 tablets suspected to contain a mixture of Testosterone Propionate (a Schedule III Controlled Substance), Tadalafil (an uncontrolled prescription medication), and Sildenafil (an uncontrolled prescription medication) destined to WEEMS at 2373 Jefferson Street, Laramie, WY 82070 (hereafter Seized Shipment 2). SA Elder requested Seized Shipment 2 be forwarded to her in Cheyenne.
37. On March 12, 2018, SA Estes received Seized Shipment 1. On March 14, 2018 SA Estes received Seized Shipment 2. On March 14, 2018 SA Estes and SA Matthew Huffman transported both seizures to the Wyoming State Crime Laboratory in Cheyenne, Wyoming for analysis. Both seizures appeared to SA Estes to contain red and green colored gel caps of similar consistency and packaging. Wyoming State Crime Lab personnel conducted testing on red capsules found within Seized Shipment 1 and Seized Shipment 2. Tested capsules

tested presumptive positive for the presence of Testosterone Propionate (a Schedule III Controlled Substance), Tadalafil (an uncontrolled prescription medication), and Sildenafil (an uncontrolled prescription medication). Green capsules from within Seized Shipment 1 and Seized Shipment 2 had been previously submitted for testing to NMS Labs, on February 22, 2018, by US Customs and Border Protection (CBP) Officers. Green capsules submitted for testing by CBP tested presumptive positive for the presence of Testosterone Propionate (a Schedule III Controlled Substance) and Sildenafil (an uncontrolled prescription medication).

38. On March 19, 2018, SA Estes received information from the Wyoming Division of Criminal Investigation (DCI) indicating Fred WEEMS is the owner and organizer of MATCHA GREEN TEA LLC, Missouri Business Charter Number LC001501582, formed August 1, 2016.
39. On November 23, 2018, SA Estes learned of another shipment of an additional approximately 47,728 tablets suspected to contain Tadalafil (an uncontrolled prescription medication) destined to WEEMS at 2373 Jefferson Street, Laramie, WY 82070 (hereafter Seized Shipment 3). SA Estes requested Seized Shipment 3 be forwarded to him in Cheyenne.
40. On November 27, 2018, SA Estes received information from the CBP National Targeting Center (NTC) personnel indicating approximately 20 packages had been sent from China to 2373 Jefferson Street, Laramie, Wyoming between October 19, 2017 and October 19, 2018. The recipients of these packages included MATCHA GREEN TEA LLC and Fred WEEMS. These packages were manifested as weighing between 1.8 pounds and 27 kilograms (approximately 52.9 pounds). The 20 packages located by NTC includes Seized Shipments 1, 2, and 3. The 20 packages were manifested as organic pigment, pigment yellow, polypropylene plastic particles, polypropylene powder, polyacrylamide, dandelion extract, crystal soil, green tea extract, and bitter melon extract. Seized Shipment 1 was manifested as

pigment yellow. Seized Shipment 2 was manifested as organic pigment. Seized Shipment 3 was manifested as dandelion extract.

41. On November 28, 2018, SA Estes received information from Wells Fargo Bank (WFB) indicating Fred WEEMS had sent and received several international wire transfers involving the Bank of China between June 25, 2018 and September 4, 2018. Information received from WFB indicated the following activity (all transactions are to or from the Bank of China):

- a wire transfer out on June 27, 2018 for \$1500.00;
- a wire transfer out on July 6, 2018 for \$5266.00;
- a wire transfer in on August 2, 2018 for \$8630.00;
- a wire transfer out on August 7, 2018 for \$7559.90;
- a wire transfer out on September 14, 2018 for \$10,890.00;
- a wire transfer out on September 19, 2018 for \$1718.54

42. On November 29, 2018 SA Estes received information from NTC personnel that a package had been sent originating in China, on or about November 29, 2018, to MATCHA GREEN TEA LLC at 2373 Jefferson Street, Laramie, Wyoming 82070 via FedEx bearing a tracking number ending in 9009. On December 3, 2018 SA Estes received information from NTC personnel indicating the package had arrived in the US and had not been inspected upon entry. On December 3, 2018 SA Estes received information from US Drug Enforcement Administration (DEA) SA Mark Lee indicating the package bearing the tracking number ending in 9009 was in Laramie, Wyoming pending delivery. SA Estes and SA Lee contacted FedEx personnel in Laramie, Wyoming and were able to locate the package bearing a tracking number ending in 9009 prior to delivery. SA Estes observed the package to be a large box weighing approximately 50 pounds with what appeared to be Chinese writing on the box. A label on the box indicated the contents to be *Tribulus terrestris* (a plant species). SA Estes conducted an Extended Border search of the package and located approximately 14 Mylar bags inside the package weighing approximately 3 pounds. SA Estes recognized these Mylar bags to have been consistent with the Mylar bags found in Seized Shipment 1 and Seized

Shipment 2. SA Estes opened one of the Mylar bags and found red gel capsules similar to those found in Seized Shipment 1 and Seized Shipment 2. SA Estes detained the package bearing a tracking number ending in 9009 pending testing of the contents. On December 4, 2018, SA Estes submitted one red gel capsule taken from the open Mylar bag within the package bearing a tracking number ending in 9009 to the Wyoming State Crime Laboratory for testing. Testing revealed the red gel capsule tested presumptive positive for the presence of Testosterone Propionate (a Schedule III Controlled Substance) and Tadalafil (an uncontrolled prescription medication). SA Estes seized the package bearing a tracking number ending in 9009 (hereafter Seized Shipment 4).

43. On December 4, 2018, SA Estes received information from NTC personnel indicating a package had been sent from China to 2373 Jefferson Street, manifested to weigh 21 kilograms (approximately 46.9 pounds) and manifested to contain hesperidin (a plant pigment used in dietary supplements).
44. On December 6, 2018, SA Estes received Seized Shipment 3 from CBP Personnel. SA Estes observed the outer box Seized Shipment 3 was packaged in to be nearly identical to the outer box Seized Shipment 4 had been packaged in.
45. On December 7, 2018, SA Estes, and other law enforcement officers, conducted a trash pull at 2373 Jefferson Street, Laramie, Wyoming, 82070. Among other items, SA Estes observed plastic bubble wrap and FedEx shipping documents to have been contained in the trash of 2373 Jefferson Street, Laramie, Wyoming 82070. The FedEx shipping documents recovered indicated a package had been to Fred WEEMS and MATCHA GREEN TEA LLC at 2373 Jefferson Street, Laramie, Wyoming 82070 bearing a tracking number ending in 9437. SA Estes queried the tracking number in 9437 in the FedEx public-facing tracking website. Information returned in the FedEx public-facing tracking website indicated this package had been sent from Shanghai, China on October 13, 2018 and delivered on October 19, 2018. The

FedEx public-facing tracking website further indicated the package weighed approximately 21.4 pounds.

46. On December 11, 2018, the US District Court for the District of Wyoming issued a search warrant for WEEMS' residence located at 2373 Jefferson Street, Laramie, Wyoming 82040 under 18SM226-R. On December 12, 2018 SA Estes and other law enforcement officers executed the above-mentioned search warrant. During the execution of the search warrant, WEEMS was interviewed and stated, among other things, that he receives and reships packages of capsules on behalf of a man he knows as LI. WEEMS stated the capsules typically arrive in large shipments on a regular basis, normally every other month and weighing approximately 20 kilograms per box. The pills arrive via FedEx and WEEMS then transports the pills to a storage unit located at Spring Creek Self Storage, 830 Boswell Drive, Laramie, Wyoming for safekeeping and repackaging prior to re-shipping. The pills were placed into bins on shelves by color. The pills were red, blue, light blue and green. WEEMS stated he receives instructions from LI as to where to ship capsules and in what amounts. WEEMS stated he also receives payment via wire transfer on behalf of LI and then forwards aggregated payments at irregular intervals. WEEMS additionally agreed to cooperate with law enforcement and communicate with LI to that end.
47. On December 29, 2018, SA Estes was notified by Fred WEEMS that three additional packages had arrived at his residence in Laramie, Wyoming from Monterey Park, California, but appeared to have originated in China. WEEMS requested SA Estes and other law enforcement examine the packages and take custody of the packages if their contents were illegal. On January 2, 2019, SA Estes, accompanied by US Postal Inspector Christopher Lucas and DEA SA Mark Lee, examined the three packages, found them to be unopened and, after obtaining confirming consent from WEEMS, found them to contain approximately 35 Mylar bags, seven labeled DR (dark red), 20 labeled DB (dark blue), four labeled G (green), and four labeled DP (dark purple). Samples from the bags labeled DB and G (green and dark blue) were submitted

for testing at the Wyoming State Crime Laboratory and tested presumptive positive for the presence of Testosterone Propionate (a Schedule III Controlled Substance), Tadalafil (an uncontrolled prescription medication), and Sildenafil (an uncontrolled prescription medication).

48. On January 3, 2019, SA Estes was contacted by WEEMS. WEEMS stated he had been contacted by LI and asked to send two shipments of capsules out. One shipment, as instructed by LI, was to be sent to Jason PHILLIPS, ADVANCED NUTRITION, at 111 Rosewood Street, Lake Jackson, Texas 77566 and consist of two bags of green capsules (approximately two kilograms of capsules).
49. On January 4, 2019, SA Estes received information from the US Postal Inspection Service that the names Jason PHILLIPS, ADVANCE NUTRITION, as well as others, receive mail at 111 Rosewood Street, Lake Jackson, Texas 77566.
50. On January 4, 2019, SA Estes conducted a check of the CLEAR database which revealed Jason PHILLIPS resides at 111 Rosewood Street, Lake Jackson, Texas 77566 and is the owner of ADVANCED NUTRITION at the same address.

#### **ANTICIPATED CONTROLLED DELIVERY**

51. On January 9, 2019, in a coordinated effort between HSI and USPS, US Postal Inspectors will deliver the package as described in paragraph 48. US Postal Inspectors will conduct a controlled delivery of a package containing the two bags of green capsules to 111 Rosewood Street, Jackson Lake, Texas 77566.
52. I anticipate that the Jason PHILLIPS or antoher occuperant will accept and sign for the package.


53. Upon delivery and acceptance of the package, I believe, based on training and experience, that located inside the residence located at 111 Rosewood Street, Jackson Lake, Texas 77566, there will be evidence as described in attachment A of this affidavit which can be used as direct evidence in criminal proceedings to demonstrate the scope and magnitude of this drug trafficking organization.

**CONCLUSION**

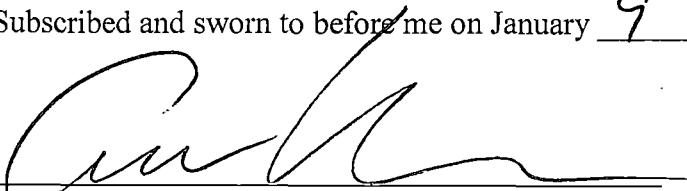
WHEREFORE, I respectfully submit that there is probable cause to believe that there is evidence as described in "Attachment B" of unlawful drug trafficking located within for 111 Rosewood Street, Lake Jackson, TX 77566. I respectfully request that the court issue warrants authorizing the search of the described property.

**END OF SWORN STATEMENT**

Respectfully submitted,

  
\_\_\_\_\_  
John Estes  
Special Agent  
DHS/ICE/Homeland Security Investigations

Subscribed and sworn to before me on January 9, 2019

  
\_\_\_\_\_  
The Honorable Andrew M. Edison  
UNITED STATES MAGISTRATE JUDGE